ASIAN LEGAL BUSINESS

MAY 2024 / ASIA EDITION

Thomson Reuters™

INSIDE

CLIENTS SELECT THE TOP OFFSHORE LAWYERS

WHAT MAKES A LEADING IN-HOUSE TEAM

UNPACKING THAILAND'S NEW DATA RULES

ASIA'S BEST FIRMS FOR PATENT, COPYRIGHT AND TRADEMARK WORK

IP RANKINGS 2024

MCI (P) 004/02/2024
ISSN 0219 – 6875
KDN PPS 1867/10/2015(025605)

ISSN 0219-6875 05
9 770219 687507

NEW DATA, NEW RULES

Thailand is one of the countries in Southeast Asia most prone to cyber vulnerabilities and data breaches. To combat that, the authorities in the past year released two subordinate regulations concerning the transfer of personal data across borders under the Personal Data Protection Act (PDPA). Lawyers in Thailand unpack the new rules and outline what businesses are required to do. **BY SARAH WONG**

Thailand has been quickly catching up with Southeast Asia's brisk pace in enhancing data protection as cross-border activities increase and cyber security threats loom larger. And companies doing businesses in the second largest ASEAN economy are staring at increasingly severe punishment for non-compliance.

In June 2022, the Personal Data Protection Act (PDPA) - Thailand's first consolidated data protection law - came into full effect after being postponed twice due to the COVID pandemic. Since then, Thailand has been actively refining its approach on safeguarding personal data and securing cross-border transfers with an emphasis on transparency and consent.

"In general, the transfer of personal data outside Thailand typically requires obtaining consent, unless the destination country has adequate personal data protection measures (known as 'adequate country'), the transfer qualifies under specific exemptions, or appropriate safeguards are in place," explain Pranat Laohapairoj, partner, and Suphakorn Chueabuncha, senior associate, at Thai law firm Chandler MHM.

However, it could be a nuisance for companies to secure permission for international data transfers during their regular activities. Business operations are subject to disruptions if consent cannot be obtained. All this has made it essential to explore alternative approaches.

In December last year, the country's Personal Data Protection Committee (PDPC) issued two subordinate regulations to address essential aspects of the cross-border transfer of personal data. The two notifications have come into effect since March.

"After a long period during which a loophole in cross-border transfer requirements existed, some operators opted to manage risks by engaging in offshore transfers without seeking exemptions," Pranat and Suphakorn point out.

"These regulations provide operators with guidance on how to navigate cross-border data transfers under the PDPA, allowing for transfers with fewer statutory hurdles while ensuring compliance with data protection requirements and facilitating international business activities," they add.

NEW SAFEGUARDS

The first notification sets out two criteria classifying whether a destination country or organisation is "adequate" in offering personal data safeguards.

To satisfy the "adequacy" test, there needs to be data protection law or regulations in place in the destination country or organisation that align with or exceed the standards of the PDPA. Those include obligations assigned to data controllers to put in place security measures to protect the rights of data subjects with enforceable legal instruments in the case of breaches.

The second criteria is to determine whether such country, subject to consideration for its adequacy, has a proper authority or organisation to enforce their regulations.

Pranat and Suphakorn tell ALB that this notification imposes a self-assessment requirement on business operators, according to a PDPC member.

"Operators must assess whether the destination country meets the adequacy criteria, assuming the associated risks themselves. Alternatively, in uncertain cases, operators may request the PDPC to make a decision on a case-by-case basis (referred to as an 'adequacy decision')," say Pranat and Suphakorn. They add that PDPC may publish a list of countries deemed adequate - known as a "whitelist", which has yet come into existence.

The second notification deals with data transfers to destination countries which fail to be seen as adequate under the PDPA, nor qualify for any derogations as stipulated in the law.

In this case, business operators are required to ensure a set of appropriate safeguards, which include implementing Binding Corporate Rules (BCR).

"In this regard, the BCR must be certified by the PDPC office based on the following three criteria: the legal effectiveness and enforceability of such BCR; clauses that recognise personal data protection, data subject's rights, and mechanisms for lodging complaints; and appropriate security measures that are in compliance with the minimum requirements prescribed by PDPA," note Pranat and Suphakorn.

In addition, operators can utilise Standard Contractual Clauses (SCC) for cross-border transfers, which is an agreement between a data exporter and

Choices Surrounding Personal Data Breach Notification

The Personal Data Protection Act B.E. 2562 ("PDPA") mandates prompt notification to the authority and/or affected data subjects in the event of a data breach. Despite this requirement, many operators have historically hesitated to report breaches due to fear of potential non-compliance with the PDPA. However, it is noteworthy that breaches are often brought to light by data subjects, who may take to social media to share their experiences or approach the authority directly without consulting with the operator first. This heightened and abrupt visibility can attract the attention of the authority and the public, potentially damaging the operator's reputation and increasing the risks of non-compliance. Although the authority has not imposed any penalties on operators, this period of leniency is coming to an end.

On the other hand, proactive reporting to the authority can lead to more favorable outcomes. The authority may request evidence demonstrating that the operator has taken reasonable steps to mitigate the risks, potentially avoiding further punitive action. Therefore, unless operators can definitively conclude that there is no risk to any data subjects, it is advisable for them to promptly notify the authority upon discovering the unfortunate occurrence. Furthermore, operators are advised to have necessary documents in place, as the lack of proper documentation may be discovered by the authority upon reporting.

1

2

*1 - **Pranat Laohapairoj**, Partner*
E: pranat.l@mhm-global.com

*2 - **Suphakorn Chueabunchai**,*
Senior Associate
E: suphakorn.c@mhm-global.com

Chandler MHM
W: www.chandlermhm.com

Data breaches can be caused not only by hackers but also by human error and natural disasters. The rule of thumb is, regardless of the cause, prompt notification to the authority and affected data subjects must be considered. If deemed necessary, operators must report the incident to the authority within 72 hours. To expedite this process, it is crucial to educate employees about data breaches and establish clear protocols for reporting incidents. Some operators have implemented internal data breach notification forms to ensure that employees can report incidents promptly and with sufficient detail. Additionally, simulating breach scenarios through workflow exercises can help prepare operators for swift and effective responses. Lastly, a common question is whether to report right away upon discovery or to wait for more information and report at a later date. The answer is that if there is probability that personal data has been accessed, a prompt notification must be undertaken to avoid any risks involving the authority.

In conclusion, operators should prioritize preparedness over fear of reporting. Timely and transparent reporting not only aligns with legal obligations but also minimizes potential damage from breaches.

a data importer designed to facilitate the safe transfer of personal data without requiring explicit approval from regulatory authorities.

The PDPC notification requires SCC to comply with the above three criteria for BCR together with some additional requirements, say Pranat and Suphakorn.

Firstly, the processing must be in compliance with the personal data protection law. Secondly, specific requirements must be complied with if a data recipient is either a data processor, or a data controller. Furthermore, the appropriate safeguards must have legal enforceability and be binding upon the related parties and ensure the rights of data subject.

"In any case, the subordinate regulation recognises two models of SCC - the ASEAN Model Contractual Clauses for Cross Border Data Flows, and the GDPR SCC - as appropriate safeguards in order to align with international practices," add Pranat and Suphakorn.

ENFORCEMENT CHALLENGES

As Thailand has upped the ante in safeguarding data privacy and cracked down on insecure cross-border data transfers, businesses are expected to operate in a safer digital environment with the reassurance of enforceable legal remedies.

However, lawyers believe the absence of the so-called whitelist and a blank history of adequacy decisions in regard to destination countries have forced business operators to take up the arduous task of evaluating the adequacy of their personal data protection measures themselves. The uncertain timeline of further PDPD announcements also adds to the complication.

"In this scenario, operators must assume the associated risks themselves," say Pranat and Suphakorn. "Under such circumstances, appropriate alternative safeguards, such as BCR and SCC, may prove to be more practical options for operators requiring cross-border transfers of personal data. These safeguards can help mitigate risks and ensure compliance with data protection regulations in the absence of recognized adequacy decisions or whitelist."

Failure to comply with the requirements and obligations under any sub-regulations issued under the PDPA could result in the penalties specified under the PDPA. The maximum fine of 5 million baht ($135,750) applies specifically to cases involving cross-border transfers of sensitive personal data, while the maximum fine for other cases is 3 million baht. That's because in instances involving cross-border transfers, enforcement may be more challenging due to difficulties in compelling compliance from data recipients located outside Thailand.

However, "when determining whether to impose an administrative fine, the relevant authority considers factors such as the severity and circumstances of the case, including the extent of damage to data subjects, the value of damages, fines historically imposed in similar cases, and the method of remedy," note Pranat and Suphakorn.